Re: Legacy SAM API Risk

1 message

Abdikadir Said - QD2-C <abdikadir.said@gsa.gov> Tue, Dec 3, 2019 at 3:43 PM
To: Uma Jayachandran - IQSE <uma.jayachandran@gsa.gov>
Cc: "Zhabaron Hall (M1ES)" <zhabaron.hall@gsa.gov>, (b) (6) @gmail.com, CJ Densmore - IQSE <calvin.densmore@gsa.gov>

Good Afternoon All,

As the ISSO, I will go with option 2, which is to remove the POC email addresses and phone numbers from the current API response. Unfortunately, we cannot put in an AoR unless it is the last possible resort to remediate the risk and I am sure (b) (5) will not be happy with that route either. If you think this work load may be too much, we need IBM to complete the AoR and security will review the justification and make the case to (b) (5). Please feel free to setup a meeting to discuss this matter further.

Thank you,

Abdikadir Said
Information System Security Officer (ISSO)
Integrated Award Environment (IAE)
US General Services Administration
1800 F St, NW
Washington, DC 20405
Cell: (b) (6)
abdikadir.said@gsa.gov

On Tue, Dec 3, 2019 at 2:30 PM CJ Densmore - IQSE <calvin.densmore@gsa.gov> wrote:

> Said and I chatted, I gave my insight. He will make the final call as Security Lead. Thanks, everyone.
>
> CJ
>
> On Tue, Dec 3, 2019 at 1:38 PM Uma Jayachandran - IQSE <uma.jayachandran@gsa.gov> wrote:
>
> > CJ and Said - Please discuss and let us know your thoughts.
> >
> > Uma.
> >
> > ---------- Forwarded message ---------
> > From: **Uma Jayachandran - IQSE** <uma.jayachandran@gsa.gov>
> > Date: Tue, Dec 3, 2019 at 1:36 PM
> > Subject: Re: Legacy SAM API Risk
> > To: Marci Eaton - QD2B <marci.eaton@gsa.gov>
> > Cc: CJ Densmore - IQSE <calvin.densmore@gsa.gov>, Zack Sionakides - QD0B <zack.sionakides@gsa.gov>, Marci Eaton <marci.eaton@gsa.gov>, Zhabaron Hall (M1ES) <zhabaron.hall@gsa.gov>, Abdikadir Said - QD2-C <abdikadir.said@gsa.gov>, <(b) (6) @gmail.com>
> >
> > Marci - Including Z, Said and Edwin from the Security team. We will review and get back you.
> >
> > Thank you.
> > Uma.
> >
> > On Tue, Dec 3, 2019 at 1:19 PM Marci Eaton - QD2B <marci.eaton@gsa.gov> wrote:
> > > CJ & Uma,

(b) (5) security team has opened an item in our risk log as follows: *Currently, the SAM API does not restrict access to registration contact information and that information* (b) (5) *. Thus, the likelihood of scammers utilizing phone/text/contract scams will increase. This item is also captured as a risk in the DS&P risk log as DSP-129.*

(b) (5) suggests that since (b) (5) , that we leave as is, (b) (5) . If we go this route, (b) (5) needs a formal ARO, attached. My preference would be for (b) (5) .

Alternatively, we could remove POC email addresses and phone numbers from the current API response. This work on top of other work before SAM can be decommissioned, (b) (5) .

Please review and advise.

--
Marci Eaton

Lead Program Manager, Business Operations | Integrated Award Environment
Office of Systems Management | Federal Acquisition Service
U.S. General Services Administration
marci.eaton@gsa.gov / (b) (6)

--
Uma Jayachandran
Director, Governmentwide Acquisition Operations Division
GSA IT/Office of the Chief Information Officer
Integrated Awards Environment PMO
General Services Administration
Work 202-219-0029
Cell (b) (6)
uma.jayachandran@gsa.gov

--
Uma Jayachandran
Director, Governmentwide Acquisition Operations Division
GSA IT/Office of the Chief Information Officer
Integrated Awards Environment PMO
General Services Administration
Work 202-219-0029
Cell (b) (6)
uma.jayachandran@gsa.gov

--
Kind regards,

CJ Densmore

General Services Administration
Integrated Award Environment (IAE)
Government Technical Program Manager
System Modernization Operations & Maintenance

phone number: (b) (6)
email: ***calvin.densmore@gsa.gov***

Acceptance of Risk (AOR) Letter Instructions

Delete these instructions from the document file once the letter is complete and ready for submission. Do not include these instructions when submitting the letter for approval.

Conditions warranting an AOR Letter:

A System Owner encounters a rare or unusual circumstance that limits or eliminates the ability to remediate an identified vulnerability. Examples are:

- Embedded software dependencies
- Commercial off-the-shelf (COTS) product update time lines
- Compatibility issues between components

Conditions NOT warranting an AOR Letter:

- Delayed or ineffective flaw remediation processes (i.e., patching)
- Insufficient out-year System Life Cycle planning (for legacy components)
- System Owner preferences not supported by Office of the Chief Information Security Officer (OCISO) guidance and policies.

When are AOR Letters Required?

- For Moderate risk vulnerabilities and findings that cannot be remediated as required.
- For Critical/Very High/High risk vulnerabilities and findings that cannot be remediated as required.

What other restrictions apply to AOR Letters?

- AOR letters must include mitigating factors, compensating controls, and any other action(s) implemented to reduce the risk to the system and its data. Justification for why the vulnerability cannot be resolved must be included.
- All AOR letters have a maximum duration of one year regardless of the risk level. Upon expiration a new AOR letter must be approved. The new AOR letter must include new/current details as to why the vulnerabilities must remain unresolved. Because the resolution is more than twelve months unresolved, the IST Director must discuss the rationale for the new AOR letter with the CISO. Evidence of this discussion (date, etc. must be documented in the AOR letter).

How are AOR Letters prepared and processed?

1. The System Owner/Custodian, Information System Security Officer (ISSO), and Information System Security Manager (ISSM) determine the need for an AOR letter.
2. The ISSO in conjunction with the ISSM prepares the AOR letter, creates an AOR ID#, and places it in the letter where the AOR ID# appears. The naming convention is listed below. NN is a sequential number of the AOR, YYYY is the current Fiscal Year, and the brackets are not part of the AOR ID#.

   AOR-NN-[System Acronym]-YYYY

3. The Director of IST coordinates the review by notifying the Chief Information Security Officer (CISO) and all stakeholders, if a review discussion is appropriate.
4. The ISSM submits the AOR letter to the Authorizing Official (AO) for approval if the risk level is Moderate.
5. Critical/Very High/High Vulnerabilities require CISO concurrence and AO approval. In this case the AOR letter is sent to the Director of ISP to obtain CISO concurrence, then it is returned to the ISSM who then sends it to the AO.

6. Approved AOR letters are part of the permanent Assessment and Authorization file maintained by the ISSO and ISSM. Approved AOR Letters must also be sent to ISP at ispcompliance@gsa.gov.

U.S. General Services Administration

MEMORANDUM FOR [Name]
[Position/Title]
Authorizing Official

FROM: [Name]
[Position/Title]
Information System Security Manager

SUBJECT: Acceptance of Risk for Select an Option Risk Vulnerabilities for [System Name] – [Short Description of Vulnerability(ies)]

DATE: Click here to enter a date.

AOR ID # AOR-NN-[System Acronym]-YYYY

I understand compliance/implementation with GSA's information security policies and standards is required for all organizational information systems. I, as the Authorizing Official, accept responsibility for the risks associated with the exceptions to GSA IT Security policies. The following attachment provides a description of the vulnerability(ies), the risks if exploited, the potential impacts, mitigating controls implemented, and the rationale for non-compliance with the required security controls and GSA information security policies and standards. Specific detailed information on the vulnerabilities may be obtained by reviewing the Security Assessment Report (SAR) and the POA&Ms of the affected systems.

X
Approval
System ISSM

X
Concurrence
Chief Information Security Officer

X
Approval
Authorizing Official

AOR-NN-[System Acronym]-YYYY	
POAM ID#	*POAM ID#*
POAM ID#	*POAM ID#*
POAM ID#	*POAM ID#*
POAM ID#	*POAM ID#*
POAM ID#	*POAM ID#*

Description of Risk

This AOR Letter expires 12 months from the approval date or sooner if any of the following activities occur in relation to the described risks: new vulnerabilities are identified, system changes or remediations are implemented, or there is a change to existing security controls.

System Information	
Host Name	
Operating System	
IP Address	
Function of the System	
Services Running on the System	
Risk Information	
Describe the hardware or software that is the source of the vulnerability.	
Provide a specific description of the vulnerability.	
List the residual risk rating for the vulnerability(ies)	
Describe specific risks, exposures (internal or external), and/ or costs which could be incurred if vulnerability were exploited.	
Describe the mitigating controls currently in place that lower the impact of the risk to the system and the GSA network.	

Describe the reasons why (include specific technical and/or business reason) identified controls cannot be complied with.	
List mitigation and remediation strategies that can be implemented to lower the impact of the risk to the system and the GSA network. Include a timeline for implementing recommended mitigations and remediation strategies.	
Describe the risk to the impacted system, project, user community, and the GSA mission if the risk is accepted and the vulnerability is not remediated.	